



Department of Homeland Security Daily Open Source Infrastructure Report for 12 May 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The Arizona Republic reports that a months-long investigation into human smuggling operations and money laundering has resulted in the arrest of 62 people; the seizure of narcotics, weapons, real estate, and vehicles; the detention of 528 undocumented immigrants; and the recovery of millions of dollars. (See item [10](#))
- Reuters reports the International Maritime Organization said on Thursday, May 11, it was reviewing new proposals to track suspect ships by satellite to fight terrorism and prevent the movement by sea of illicit material such as weapons of mass destruction. (See item [16](#))
- The Union-Tribune reports two boxes containing up to 600 sticks of dynamite were found on Wednesday, May 10, in a Riverside, California, fire station driveway, prompting road and freeway ramp closures and the lockdown of a nearby school. (See item [41](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *May 11, Reuters* — **Oil tanker explodes off Philippine coast.** A small oil tanker exploded off the Philippine coastline, west of Manila, on Thursday, May 11, but the ship was not carrying a cargo of fuel, the local governor said. Eric Locsin, a terminal operations officer, said that they

were still investigating the cause of the explosion. Enrique Garcia, governor of Bataan province, said the ship was on its way to the Philippines' largest oil refiner, Petron Corp, when the explosion occurred. Media reports said two crew members were critically injured but the fire was under control. Petron has a 180,000-barrel-per-day oil refinery in Limay, Bataan province, which is around 87 miles from Manila. Locsin said the ship was waiting to be loaded with oil which was going to be distributed to the central Philippines and the southern island of Mindanao.

Source: http://news.scotsman.com/latest_international.cfm?id=7048820_06

2. *May 10, Reuters* — **U.S. oil executive shot dead in Nigeria; three foreign oil workers kidnapped.** A gunman on a motorcycle shot dead a U.S. oil executive in an apparently planned assassination in the city of Port Harcourt in Nigeria's oil heartland on Wednesday, May 10, authorities said. The Movement for the Emancipation of the Niger Delta (MEND), militants who have been waging a five-month-long campaign against the oil industry, denied any involvement in the killing of the executive, who worked for Texan oil services company Baker Hughes. The attack adds to a trend of rising violent crime in the vast wetlands region, which pumps all of the nation's oil. Three foreign oil workers, including one Italian, were also kidnapped from a car under armed escort in Port Harcourt on Thursday, May 11, a day after a U.S. oil executive was shot dead there. MEND said it was not involved in the kidnapping.

Additional information was found at:

<http://www.washingtonpost.com/wp-dyn/content/article/2006/05/11/AR2006051100421.html>

Source: http://news.yahoo.com/s/nm/20060510/ts_nm/nigeria_killing_dc_6

3. *May 10, Register (UK)* — **Gas pump thieves go hi-tech.** Tech-savvy thieves have worked out a means to obtain free gas after hacking into electronically-controlled gas pumps. Two gas stations in St Louis, MO, report recently losing up to \$10,000 each through the scam. Crooks reportedly reprogrammed internal keypads to dispense free gas after opening up pumps. Subsequently, other unscrupulous customers take advantage of the ruse to avoid paying for gas either. "They (the thieves) have a key to the pump and then after they open up the pump they go in and they reprogram the pump, so they can have free gas. And then everybody behind them sees what they're doing, and they continue," Kevin Tippit, manager of the Phillips 66 gas station said. Amjad Darwish, owner of Mobile Food Mart, which houses another gas station, suffered a similar attack last month.

Source: http://www.theregister.co.uk/2006/05/10/gas_station_rip-off/

4. *May 09, KATU News 2 (OR)* — **Crews are preparing for the Trojan tower demolition.** On Sunday, May 21, history will be made when the cooling tower at the old Trojan power plant along the Columbia River in Oregon is brought down. More than 3,300 holes have been drilled into the concrete that will be filled with a nitroglycerin-based dynamite. Doug Loizeaux with Controlled Demolition, Inc., said: "Cooling towers have been taken down all over the world...But this is the largest one that's ever been taken down and it's the only one that has a double reinforcing mat." The walls were built extra thick so they could withstand an earthquake and it will take 2,500 pounds of explosives to bring them down. The tower will come almost straight down, 150 feet off center, and far away from the radioactive spent fuel rods that are still stored at the site. The demolition is expected to take 14 seconds.

Source: <http://www.katu.com/team2/story.asp?ID=85756>

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

5. *May 10, ABC News (FL)* — **Overtaken tanker halts traffic near Florida port.** An overturned tanker caused some big trouble near the port of Tampa, FL. As much as 6,000 gallons of molten sulphur had to be removed and transported away. The situation prompted traffic diversion.

Source: <http://www.abcactionnews.com/stories/2006/05/060510tanker.shtml>

[\[Return to top\]](#)

Defense Industrial Base Sector

6. *May 10, Aerospace Industries Association* — **Aerospace industry and DoD plan to work together on Berry Amendment changes.** Senior leaders of the Department of Defense (DoD) and the aerospace industry met last week to discuss needed changes to the specialty metals provisions of the Berry Amendment. They reached agreement in principle on changes to the Berry Amendment that will protect the specialty metals producers while also protecting the thousands of small businesses that support the DoD. The Berry Amendment restricts DoD from acquiring a number of items, including food, clothing, fabrics, and certain tools that are not produced in the U.S. The aerospace and defense industry is impacted by provisions that apply to specialty metals.

For more information on the Berry Amendment:

<http://www.aia-aerospace.org/issues/subject/subject.cfm>

Source: http://www.aia-aerospace.org/aianews/pr_detail.cfm?Content_ID=241

7. *May 10, Government Computer News* — **For warfighters, the more information the better.** Network-centric warfare and the Global Information Grid (GIG) are all about getting information to where warfighters need it, said Anthony Montemarano, director of the Defense Information Systems Agency's Information Assurance/NetOps programs. The NetOps program is a component of network-centric warfare that focuses on using commercial best practices to operate, manage and defend the GIG. The GIG has to be thought of as a weapon system, with the same command and control. "We've got to make our data machine agnostic, so you can harvest that data and create your own user defined operational picture," Montemarano said.

Source: http://www.gcn.com/online/vol1_no1/40716-1.html

[\[Return to top\]](#)

Banking and Finance Sector

8. *May 11, Computing (UK)* — **New crackdown on cyber crime in UK.** The UK's new FBI-style crime fighting agency has unveiled plans to get tough on cyber crime. The Serious Organized Crime Agency (Soca) has announced a range of new measures to tackle online crime gangs, such as a science laboratory to research emerging technologies that criminals might

exploit. The agency says it is looking to shut down organized crime gangs that use the Internet for extortion, fraud, hacking, and virus writing. It is also working with electronic payments firms and overseas law enforcement groups to target Websites trading stolen credit cards. Criminals who design, sell, or use malicious software — such as viruses, keyloggers and phishing e-mails — will also be tracked more fervently through joint operations involving Soca, the FBI, and Russia's Department K computer crime unit. Sharon Lemon, deputy director of e-crime said serious focus will be given to card-not-present fraud, which increased by 21 percent last year. Soca will work with retailers to alert them to new tactics used to hack into customer payment card databases.

Source: <http://www.itweek.co.uk/computing/news/2155797/crackdown-cyber-crime>

9. *May 11, NBC 10 (PA)* — **Skimming artists steal from Delaware Bank customers.** Police are trying to nab crooks engaged in skimming from Delaware Bank ATMs. Police said the crooks placed a small digital card skimmer over the mouth of an ATM machine. When Wilmington Trust customers put their cards in, their data was skimmed out. The crooks mounted a small camcorder above the ATM to watch customers' fingers type in PIN numbers. Police said 140 customers lost about \$80,000.

Source: <http://www.nbc10.com/money/9196414/detail.html?rss=phi&psp=news>

10. *May 10, Arizona Republic* — **Authorities arrest 62 in smuggling, money-laundering probe.** Authorities announced Wednesday, May 10, that a months-long investigation into human smuggling operations and money laundering has resulted in the arrest of 62 people, the seizure of narcotics, weapons, real estate and vehicles, the detention of 528 undocumented immigrants, and the recovery of millions of dollars. Arizona Attorney General Terry Goddard and Phoenix Police and state Department of Public Safety officials said that a Financial Crimes Task Force in March began intensive investigations into multiple criminal enterprises. Through surveillance and undercover operations, investigators found evidence of organizations involved in illegal money-making schemes.

Source: <http://www.azcentral.com/news/articles/0510bust10-ON.html>

11. *May 10, Agence France-Presse* — **Bush creates task force to fight identity theft.** President George W. Bush on Wednesday, May 10, announced the creation of a top-level task force to combat what he called "horror stories" associated with the rapidly growing crime of identity theft. "Identity theft is a serious problem in America," the president said. Identity theft affected some 3.6 million U.S. households — or about three percent of the total in the U.S. — over a six-month period in 2004, according to a U.S. Justice Department report issued last month. The estimated loss in those six months was about \$3.2 billion, or an average of \$1,290 per household. Bush also called attention to new U.S. laws cracking down on convicted identity thieves, imposing stiffer fines, and prison terms. U.S. Attorney General Alberto Gonzales said he, along with Federal Trade Commission chairwoman Deb Majoras, will co-chair the panel tasked with fighting identity theft.

White House Fact Sheet: The President's Identity Theft Task Force:

<http://www.whitehouse.gov/news/releases/2006/05/20060510-6.html>

Remarks by President Bush after meeting with victims of identity theft:

<http://biz.yahoo.com/prnews/060510/dcw066.html?v=35>

Statement of Treasury Secretary John W. Snow On Protecting Americans from Identity Theft:

<http://www.ustreas.gov/press/releases/js4249.htm>

Source: <http://www.physorg.com/news66496317.html>

12. *May 10, Finextra* — **Citibank Japan hit by systems glitch.** Citibank says a computer glitch at its Japanese branches has caused more than a quarter million incorrect transactions over the past week. The problem affected withdrawals and deposits made between Tuesday, May 2 and Monday, May 8. In some cases, transactions were recorded in accounts twice, while in others the transactions were processed but did not appear in statements. The glitch affected yen savings, U.S. dollar savings, checking, international loan card, and advanced money accounts. The botch-up was apparently caused by an incorrect batch process that occurred after implementation of a new system. Citibank says it is "taking necessary measures to prevent future occurrence".

Source: <http://finextra.com/fullstory.asp?id=15294>

13. *May 10, INQ7.net (Philippines)* — **Phishing attack targets Metrobank online bank users.** Online customers of Philippine-based Metropolitan Bank and Trust Co. (Metrobank) are being targeted by a new phishing scam. An e-mail from "Metrobank Authority" invites e-banking account holders to join a lottery by providing their customer ID (username) and password to specified Websites. The e-mail urges recipients of the e-mail message to go to two Websites, where they are asked to enter confidential information. Internet security lead analyst of the Philippine Honeynet Project Mark Ryan Talabis described the phishing attack as a "crude attempt." Talabis said that the IP addresses included in the spurious Metrobank e-mail message were traced to computer servers hosted in Beijing, China, under Net-Infinity Technology Department Ltd.

Source: http://news.inq7.net/infotech/index.php?index=1&story_id=753_50

[[Return to top](#)]

Transportation and Border Security Sector

14. *May 11, Associated Press* — **Florida's I-95 to be closed for days.** Falling trees caused by brush fires have forced the indefinite closure of a 12-mile stretch of Interstate 95, the East Coast's main traffic artery, authorities said. Smoke from several fires around the state has periodic morning closures Wednesday, May 10. Florida Highway Patrol trooper Kim Miller said I-95 will be closed from Port Orange to Edgewater likely for at least several days as crews work to clear the debris. "What's happened is that the root bulbs have burned so that the trees are now unstable and are falling into the roadway," Miller said. Eighty-four wildfires were still burning in the state Thursday morning on more than 36,800 acres, according to the state Division of Forestry. The fires along I-95 south of Daytona Beach have burned at least three homes and been blamed for dozens of accidents, including four car-wreck deaths.

Source: <http://www.cnn.com/2006/US/05/11/brush.fires.ap/index.html>

15. *May 11, Guardian (UK)* — **Irish radio sermons risk flights.** Pilots on transatlantic flights had been complaining for months about mysterious bursts of static on their cockpit radios as they approached the Dublin, Ireland airport. Now officials have revealed that it could be religious services. A lengthy investigation by ComReg finally pinpointed the source: mass services beamed out to parishioners who were housebound or who simply enjoyed listening to their

priest in their own living rooms. Priests at three churches in Counties Kildare, Meath, and Kilkenny have been warned by Ireland's communication regulator, ComReg, that unlicensed broadcasts of religious services are cutting across vital air-traffic control links. "None of the pilots actually reported hearing prayers or hymns coming over the airwaves," said Lilian Cassin, of the Irish aviation authority, "but what prompted our suspicion was the regular timings of the disturbances. Our controllers couldn't hear the static on the ground."

Source: <http://www.guardian.co.uk/international/story/0,1771999,00.html>

16. *May 11, Reuters* — **Satellites may track ships to fight terrorism.** The UN's International Maritime Organization (IMO) — the world's supreme maritime body — said on Thursday, May 11, it was reviewing new proposals to track suspect ships by satellite to fight terrorism and prevent the movement by sea of illicit material such as weapons of mass destruction. The IMO said the draft proposal, drawn up to enhance marine security, would be one of the items discussed at a 10-day meeting that began this week at its headquarters in London.

"Long-Range Identification and Tracking (LRIT) of ships has lots of other potential uses, but in this case it is being looked at as part of the wider security issue," an IMO spokesperson said. "You could also track a merchant vessel that was quite legitimately carrying a cargo that could be dangerous if it fell into the hands of terrorists." Since the September 11, 2001, attacks on the United States the maritime industry has been subject to a raft of security laws. These include the comprehensive International Ship and Port Security (ISPS) code that came into force in July 2004. Under the new proposals, merchant ships would be required to transmit through satellite-based technology their identity, location, and date and time of the position.

Source: <http://www.defensenews.com/story.php?F=1767273&C=landwar>

17. *May 11, Dallas Morning News* — **An airport flight-sharing plan.** Williams Gateway Airport near Mesa, AZ, is taking passengers and flights away from Phoenix's Sky Harbor International Airport. Phoenix's response? Invest in Williams, the converted former Air Force base that's likely to emerge as the region's second major passenger airport because it's tucked near much of the region's hottest residential growth. "There's going to be plenty of passengers for both of us," said Paul Blue, Sky Harbor's director for business and properties. The greater Phoenix region's population of 3.6 million is expected to jump to six million by 2025. Phoenix's choice reflects a counterpoint to the argument that a region should concentrate its commercial flying at a single facility, as some say North Texas should do at Dallas/Fort Worth International Airport. A campaign that Southwest Airlines Co. launched in November 2004 to lift Wright amendment restrictions at Dallas Love Field has sparked a major battle in North Texas over the future of the region's airports. According to the thinking in Phoenix, a region should invest in multiple commercial airports under a single authority to accommodate growth for decades to come and the inevitable road traffic that follows

Source: http://www.dallasnews.com/sharedcontent/dws/bus/stories/DN-p_hoenix_08bus.ART.State.Edition1.e2beba8.html

18. *May 11, Baltimore Sun* — **Cruise ship terminal opens in Locust Point.** Maryland State officials unveiled a new \$13 million cruise ship terminal along the South Locust Point shoreline on Wednesday, May 10. "Our customers will no longer have to drive around Dundalk Marine Terminal dodging trucks and loading materials," Governor Robert L. Ehrlich Jr. said during a ribbon-cutting ceremony. Unlike the former terminal in Dundalk, the new location doesn't have to share port space with cargo operations. An old lumber facility has been converted to a

60,000–square–foot cruise terminal with ticketing counters, security screeners, snack bar, and bathrooms. Parking is available for 500 vehicles, with drop–off and pickup areas at the entrance. State officials hope the new terminal will help Maryland become a larger player in the cruise business. About 30 cruises to Bermuda and the Caribbean are scheduled to depart Baltimore this year. The first, Royal Caribbean's *Grandeur of the Seas*, leaves tomorrow for a trip to the Caribbean. "This might very well be the beginning of a new era for cruising in Maryland," said F. Brooks Royster III, executive director of the Maryland Port Administration. State officials also liked the site because it's visible from Interstate 95 and not far from Baltimore–Washington International Thurgood Marshall Airport and the city's Inner Harbor. Source: <http://www.baltimoresun.com/business/bal-bz.cruise11may11.0.1180799.story?coll=bal-business-headlines>

19. *May 11, Canadian Press* — **Grenade–shaped belt buckle causes evacuation at Canadian airport.** A belt buckle shaped like a hand grenade led to the evacuation of a section of St. John's International Airport on Thursday, May 11. Bob Nurse, a security official at the airport, says an X–ray machine picked up a suspicious item inside a checked bag. A bomb squad from the Royal Newfoundland Constabulary was called in and the belt eventually found. The airport was back in normal operations after about 90 minutes.

Source: <http://www.azcentral.com/news/articles/0511BeltBuckle11-ON.h tml>

20. *May 11, Star–Ledger Times (NJ)* — **Israeli airline gains control over screening.** The Israeli airline El Al has been routinely scanning its own checked luggage for bombs and bypassing U.S. screeners at four major airports, a procedure it now wants to use at Newark Liberty International Airport. Under an unusual arrangement given to no other airline, El Al has refitted U.S. bomb–detection machines at the four airports with its own computer software, which is "more sensitive" to detecting explosives, said Amy von Walter, a Transportation Security Administration (TSA) spokesperson. The four airports are John F. Kennedy International in New York, Los Angeles International, Miami International, and O'Hare International in Chicago. The arrangement, which also allows El Al Airlines to use its own screening personnel, points to a continuing problem in the U.S.'s ability to safeguard commercial airliners. Since the September 11, 2001, terror attacks, undercover tests at U.S. airports, including Newark Liberty, have consistently shown that TSA screeners miss a significant number of fake explosives. U.S. aviation officials have repeatedly said passengers' privacy rights, as well as the sheer volume of planes, make it impossible to operate security as rigorously as El Al, which runs far fewer flights.

Source: <http://www.nj.com/news/ledger/index.ssf?/base/news-6/1147324584193820.xml&coll=1>

[\[Return to top\]](#)

Postal and Shipping Sector

Nothing to report.

[\[Return to top\]](#)

Agriculture Sector

21. *May 11, Treasure Coast Palm (FL)* — **Florida citrus crop may be quarantined.** A state official says the U.S. Department of Agriculture may soon announce a statewide citrus quarantine, which would prohibit the shipment of Florida citrus products to other citrus-producing states. "The Florida Department of Agriculture wants to have area quarantines which would allow shipment of citrus products from areas that are not impacted by greening or canker and therefore would not be quarantined," said Liz Compton, a spokesperson for the Florida Department of Agriculture and Consumer Services. "It is currently an ongoing discussion and no final decision has been made." Most citrus producing counties on the east coast of Florida, including St. Lucie, Martin and Indian River counties, have the bacterial disease canker.
Greening disease information: <http://ipm.ifas.ufl.edu/agricultural/fruit/citrus/ASP-hoy.htm>
Canker information: <http://www.biotech.ufl.edu/PlantContainment/canker.htm>
Source: http://www.tcpalm.com/tcp/local_news/article/0.2545.TCP_1673_6_4688878.00.html
22. *May 11, USAgNet* — **Canada ends search for cattle in mad cow case.** The search for cattle connected by birth or sources of feed with Canada's latest mad cow case has ended and all tests so far have been negative, officials said on Monday, May 8. The Canadian Food Inspection Agency said it has tested 12 cattle potentially exposed to the same feed as a six-year-old dairy cow found with the disease last month in British Columbia, and 11 more will be tested shortly. The 23 cattle were among 146 identified as "feed cohorts" or as offspring of the affected cow. Of the 146 cattle, 74 were already dead, 15 had been exported to the U.S. and 34 were deemed untraceable due to a lack of information.
Source: <http://www.usagnet.com/story-national.cfm?Id=872&yr=2006>
23. *May 11, Vietnam News Agency* — **Vietnam government calls for urgent foot and mouth disease control measures.** Drastic measures should be taken to promptly quarantine, control and stamp out foot and mouth disease (FMD), said Vietnam's Permanent Deputy Prime Minister Nguyen Tan Dung. Dung chaired a meeting with relevant ministries and services in Ha Noi on May 11 to discuss measures to prevent and combat the disease. Since early this year, the Prime Minister has approved a five-year program to prevent and combat FMD with funding of 250 billion (VND) in order to eliminate the disease by 2010. FMD has affected nearly 10,000 cattle and over 12,000 hogs in 130 communes and wards in 74 districts of 21 provinces and cities.
Source: http://www.vnagency.com.vn/NewsA.asp?LANGUAGE_ID=2&CATEGORY_ID=29&NEWS_ID=198709

[\[Return to top\]](#)

Food Sector

Nothing to report.

[\[Return to top\]](#)

Water Sector

24.

May 11, Record (CA) — **California has concerns over Lodi's wastewater facility.** Lodi, CA, officials have received notice from state regulators that the city's wastewater treatment plant wasn't adequately testing treated effluent and was in violation of state rules. But the May 3 letter to Public Works Director Richard Prima also warned Lodi that state officials are concerned the White Slough plant is harming groundwater. The violation notice, which stems from a November 21 inspection, orders Lodi to submit a plan outlining how it intends to meet the requirements. Water board inspectors found that Lodi stopped checking for chlorine in discharged water after the city switched from chlorine to an ultraviolet disinfection system on January 21, 2005; did not retest water samples when the first tests failed to work properly; and did not increase monitoring when water samples reached potentially toxic levels.

Source: <http://www.recordnet.com/apps/pbcs.dll/article?AID=/20060511/NEWS01/605110322/1001/NEWS01>

25. *May 11, Gwinnett Daily Post (GA)* — **Road work causes large sewer spill.** On Monday, May 8, a contractor hired to fortify a massive sewer line damaged it, sending 30,000 gallons of raw sewage into Sweetwater Creek in Lawrenceville, GA. County workers staunched the flow within four hours, but not until Tuesday night was the 42-inch thick line repaired, allowing the sewer system to resume its normal operation. In the interim, the county had to divert sewage to other pipes and treatment plants. The incident happened when workers were installing a concrete platform over the pipe to ensure it can withstand the weight of dirt being dumped there for a road project.

Source: http://www.gwinnettdailypost.com/index.php?s=&url_channel_id=32&url_article_id=14930&url_subchannel_id=&change_well_id=2

26. *May 10, WGAL (PA)* — **Officials keep eye on water supply after chemical spill.** Water company officials are monitoring the Sheppard–Meyers reservoir in York, PA, for contamination after a chemical spill Tuesday, May 9. A farm truck overturned, spilling several gallons of liquid fertilizer and herbicide near the reservoir in West Manheim Township. The water company does not think the reservoir is contaminated.

Source: <http://www.wgal.com/news/9190733/detail.html>

[[Return to top](#)]

Public Health Sector

27. *May 12, Agence France–Presse* — **Thirteen companies agree to drop single–drug malaria treatment.** Thirteen pharmaceutical companies have agreed to stop selling anti–malarial drugs based solely on the recently discovered artemisinin compound, the World Health Organization (WHO) said. The move follows an appeal by WHO in January, amid signs in Asia that single–drug treatment could help malaria parasites develop resistance to artemisinin. The compound, which helps the body ward off malaria but does not kill the parasite, was developed in recent years because the mosquito–borne parasite has developed resistance to traditional anti–malarial drugs. WHO says that artemisinin is nearly 95 percent effective in curing uncomplicated malaria when used in combination therapy with other anti–malarials. The agreement includes the major manufacturers of artemisinin monotherapy drugs, said WHO. About ten other companies are being monitored.

Malaria information: <http://www.who.int/topics/malaria/en/>

Source: <http://www.todayonline.com/articles/117977.asp>

28. *May 11, New York Times* — **Hepatitis risk for East Asians in New York.** Among east Asian immigrants in New York City, one person in seven carries the hepatitis B virus, a new study has found. The study, led by researchers at New York University School of Medicine, found that 15 percent of east Asians in New York — as many as 100,000 people — are chronic hepatitis carriers, with the rate highest among immigrants from China. That infection rate is 35 times the rate found in the general population. Because Hepatitis B is endemic in many Asian countries, growth in the number of Asian immigrants in New York and across the country has made the disease a broad, expensive, emerging health problem. In the 2000 census, there were 800,000 Asians in the city, with roughly half from China. Hepatitis B, like hepatitis C, is generally contracted through the blood, and is not transmitted through casual contact with infected people. "The health care costs are enormous," said Dr. Henry J. Pollack, the lead author of the study. "If you're giving what would be considered to be the proper care for all these people, it would be hundreds of millions of dollars."

Study: <http://www.cdc.gov/mmwr/preview/mmwrhtml/mm5518a2.htm>

Source: <http://www.nytimes.com/2006/05/11/nyregion/11hepatitis.html?ex=1147406400&en=fa03ace49a14701c&ei=5087%0A>

29. *May 11, Agence France–Presse* — **Djibouti reports first human case of deadly bird flu in east Africa.** The tiny Red Sea state of Djibouti reported east Africa's first human case of the H5N1 bird flu strain and said some chickens were also infected. The health ministry said that virology tests from samples of an infected person taken last month were positive for the virulent strain of the flu virus, which had also affected three domestic fowl. The ministry said the tests were carried out with the collaboration of the World Health Organization (WHO). Djibouti is the first country in east Africa to report the appearance of the H5N1 virus in either birds or humans and the second in Africa to report a human case after Egypt. It is the eighth African country to find the strain in birds after Nigeria, Egypt, Niger, Cameroon, Burkina Faso, Ivory Coast and Sudan.

Source: http://news.yahoo.com/s/afp/20060511/hl_afp/healthfludjibouti_060511160459

30. *May 11, Associated Press* — **U.S. wants more tests of anthrax vaccine.** VaxGen Inc. said Wednesday, May 10, that the federal government was demanding that the biotechnology company conduct more human tests before delivering a new anthrax vaccine. It is the second delay since the company won the \$877.5 million contract in 2004. The contract was the first awarded under Project BioShield, a law President Bush signed in 2004 that promises \$5.6 billion to develop remedies against bioweapons.

Source: <http://www.latimes.com/business/la-fi-vaxgen11may11.1.1631474.story?coll=la-headlines-business>

[[Return to top](#)]

Government Sector

31. *May 11, Associated Press* — **Powdery substance prompts evacuation of Indianapolis City–County Building.** The Marion County Health Department is analyzing a powdery

substance that prompted the evacuation of the City–County Building in Indianapolis on Wednesday evening, May 10. A Marion County Sheriff's Deputy, a property room clerk and an Indianapolis firefighter were exposed to the powder, but were not seriously injured. Deputy Sean Morrison found packets of the powder on a suspect. When he touched the substance in the property room, he had a reaction that included redness in his eyes, muscle pain, sweating, and lowered blood pressure.

Source: <http://www.wishtv.com/Global/story.asp?S=4884059&nav=0Ra7>

[\[Return to top\]](#)

Emergency Services Sector

32. *May 10, KKTV (CO)* — **Colorado hosts Chemical Stockpile Emergency Preparedness Program exercise.** Nearly 1,000 people from local, state and federal agencies participated in an exercise Wednesday, May 10, to test emergency response capabilities in Pueblo County, CO. The exercise tested the capabilities of fire, hazardous materials teams, law enforcement, schools, emergency medical, victims assistance, health and environmental, area non–profit, emergency management and other agencies. This federally managed and evaluated exercise was sponsored by the Chemical Stockpile Emergency Preparedness Program (CSEPP). The CSEPP event occurred at the U.S. Army Pueblo Chemical Depot and tested notification procedures, communications, emergency public information and emergency response capabilities.

Source: <http://www.kktv.com/home/headlines/2775736.html>

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

33. *May 10, Security Focus* — **Verisign i–Nav ActiveX control remote buffer overflow vulnerability.** Verisign i–Nav ActiveX control is prone to a buffer overflow vulnerability. The software fails to perform sufficient bounds checking of user supplied input before copying it to an insufficiently sized memory buffer. Analysis: This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of the Verisign i–Nav ActiveX control. User interaction is required to exploit this vulnerability in that the target must visit a malicious Webpage. The specific flaw exists within the "VUpdater.Install" ActiveX control which is used to provide native support for Internationalized Domain Names in Microsoft Internet Explorer, Microsoft Outlook and Microsoft Outlook Express.

Solution: Reportedly, the vendor has released updated versions of the affected software to address this issue. Users of affected packages should contact the vendor for further information.

For more information: <http://www.securityfocus.com/bid/17939/references>

Source: <http://www.securityfocus.com/bid/17939/discuss>

34. *May 10, Security Focus* — **Cisco Application Velocity System open TCP proxy vulnerability.** Cisco Application Velocity System (AVS) is susceptible to a remote open TCP proxy vulnerability. Analysis: The AVS may be used to forward unexpected traffic and to obscure the true originator of undesirable traffic. This issue allows remote attackers to utilize

the affected software as an open TCP proxy. This has been exploited by attackers to send unsolicited commercial e-mail.

Vulnerable: Cisco Application Velocity System 3120 5.0; Cisco Application Velocity System 3110 5.0; Cisco Application Velocity System 3110 4.0.

Solution: Cisco has released an advisory, along with fixes to address this issue. Please see the referenced advisory for further information. It should be noted that the advice given in the workaround section must still be performed once fixes have been applied:

<http://www.securityfocus.com/bid/17937/references>

Source: <http://www.securityfocus.com/bid/17937/discuss>

- 35. *May 10, Security Focus* — Microsoft Windows path conversion weakness.** Microsoft Windows is susceptible to a path conversion weakness that may allow attackers to bypass security applications. Analysis: This issue is due to the operating system utilizing multiple differing file path resolution algorithms. This allows the exploit by attackers to bypass security software such as anti-virus and anti-spyware software. Other attacks may also be possible. Any software utilizing the affected function, or utilizing APIs and other functions that in turn utilize the affected function may be affected by this issue. Specific information regarding affected software and versions is known to be incomplete and possibly inaccurate.

For a complete list of vulnerable products: <http://www.securityfocus.com/bid/17934/info>

Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

Source: <http://www.securityfocus.com/bid/17934/references>

- 36. *May 10, Security Focus* — Microsoft Internet Explorer position CSS denial-of-service vulnerability.** Microsoft Internet Explorer is affected by a denial-of-service vulnerability. Analysis: This issue arises because the application fails to handle exceptional conditions in a proper manner. An attacker may exploit this issue by enticing a user to visit a malicious site, resulting in a denial-of-service condition in the application.

For a complete list of vulnerable products: <http://www.securityfocus.com/bid/17932/info>

Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

Source: <http://www.securityfocus.com/bid/17932/discuss>

- 37. *May 10, FrSIRT* — Microsoft Windows Infotech Storage System Library heap corruption vulnerability.** A vulnerability has been identified in Microsoft Windows, which could be exploited by attackers to execute arbitrary commands. Analysis: The heap corruption error in the Infotech Storage System Library ("itss.dll") does not properly handle malformed ".CHM" files, which could be exploited by attackers to compromise a vulnerable system by tricking a user into opening or decompiling a malicious ".chm" file using the Microsoft Windows Help Utility ("hh.exe").

Affected products: Microsoft Windows 2000 Service Pack 4; Microsoft Windows XP Service Pack 1; Microsoft Windows XP Service Pack 2.

Solution: The FrSIRT is not aware of any official supplied patch for this issue.

Source: <http://www.frsirt.com/english/advisories/2006/1761>

- 38. *May 10, Tech Web* — Users report glitches with Microsoft's Flash Patch.** If, as an analyst suggested Tuesday, May 9, Microsoft plans to begin patching more than its own software, its first effort got off to a rocky start. By Wednesday, May 10, Windows users were complaining of glitches in updating Adobe's Flash Player through the Windows Update service. Microsoft

took the unusual step Tuesday of feeding an updated edition of Flash Player to Windows XP, Windows 98, and Windows Millennium users. It was the first time the Redmond, WA, developer took an active role in pushing a third-party product update to users. Microsoft is aware of the problem, which it dubbed a "known issue" in a support document posted Wednesday. The document offers a workaround that requires users to delete a pair of Flash-related files, then manually download and install the Player update.

Source: <http://www.informationweek.com/news/showArticle.jhtml?articleID=187202029&subSection=Breaking+News>

39. *May 08, Federal Computer Week* — **Industrial control systems pose little-notice security threat.** The electronic control systems that act as the nervous system for all critical infrastructures are insecure and pose disastrous risks to national security, cybersecurity experts warn. Supervisory control and data acquisition and process control systems are two common types of industrial control systems that oversee the operations of everything from nuclear power plants to traffic lights. Their need for a combination of physical security and cybersecurity has largely been ignored, said Scott Borg, director and chief economist at the U.S. Cyber Consequences Unit, an independent research group funded by the Department of Homeland Security. Control systems security is one of six areas of critical vulnerabilities Borg included in a new cybersecurity checklist released in April by the research group. The private-sector owners of critical infrastructure refuse to release data and deny that their aging, inherently insecure systems pose any security risk, said Dragos Ruiu, an information technology security consultant to the U.S. government who runs several hacker conferences. Average hackers can break into the systems, said Robert Graham, chief scientist at Internet Security Systems. He, Borg and other experts fear that major cyberattacks on control systems could have socio-economic effects as severe and far-reaching as Hurricane Katrina.
- Source: <http://fcw.com/article94273-05-08-06-Print>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT is aware of publicly available, working exploit code for an unpatched vulnerability in Oracle Export Extensions. Successful exploitation may allow a remote attacker with some authentication credentials to execute arbitrary SQL statements with elevated privileges. This may allow an attacker to access and modify sensitive information within an Oracle database.

More information about this vulnerability can be found in the following:

Secunia Advisory19860

<http://secunia.com/advisories/19860>

Security Focus Oracle Vulnerability Report

<http://www.securityfocus.com/bid/17699/discuss>

Red Database Security Oracle Exploit Report

http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html

US-CERT recommends the following actions to mitigate the security risks:

Restrict access to Oracle:

Only known and trusted users should be granted access to Oracle. Additionally, user accounts should be granted only those privileges needed to perform necessary tasks.

Change login credentials for default Oracle accounts:

Oracle creates numerous default accounts when it is installed. Upon installation, accounts that are not needed should be disabled and the login credentials for needed accounts should be changed.

Oracle has released Critical Patch Update April 2006. This update addresses more than thirty vulnerabilities in different Oracle products and components.

http://www.oracle.com/technology/deploy/security/pdf/cpuapr2_006.html

Phishing Scams

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US-CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT.

http://www.us-cert.gov/nav/report_phishing.html

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

Current Port Attacks

Top 10 Target Ports	1026 (win-rpc), 6881 (bittorrent), 25 (smtp), 445 (microsoft-ds), 41170 (---), 50497 (---), 49200 (---), 6588 (AnalogX), 135 (epmap), 5817 (---) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	---

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

40. *May 11, Tonganoxie Mirror (KS)* — **Spill leads to grade school evacuation.** For the second time in less than a month, Tonganoxie Elementary's students and staff participated in a disaster drill. But Tuesday morning, May 9, it wasn't for practice. School officials evacuated the building because of the discovery of an unknown substance within the building. "We received a shipment of a couple of computer monitors," said assistant principal Tammie George. "When our computer tech, Jim Moody, was opening the boxes, there was some kind of a liquid and when he touched it, it created kind of a burning sensation." Moody followed the district's procedure for a chemical spill and alerted school officials. "We found out it was just a chemical from the monitor itself," George said. "We took the necessary precaution to remove students from that wing of the building and then evacuated the entire building for a short period of time." Meanwhile, George said the experience of running through a disaster drill was a chance to see how things could work in the event of an unexpected emergency.

Source: http://www.tonganoxiemirror.com/section/frontpage_lead/story/9176

[[Return to top](#)]

General Sector

41. *May 11, Union-Tribune (CA)* — **Boxes thought to be dynamite prompt lockdown, road closures.** Two boxes believed to contain dynamite were found in Riverside, CA, on Wednesday, May 10, in a city fire station driveway, prompting road and freeway ramp closures and the lockdown of a nearby school, according to a police and on-scene reports. The black boxes were found in front of Fire Station No. 6 at 2293 Main St., near downtown, said Steven Frasher of the Riverside Police Department. The police department's bomb squad was sent to the scene, along with agents from the federal Bureau of Alcohol, Tobacco, and Firearms. "It's been inspected. It's been determined to be an explosive package," Frasher said. Local news reported that the boxes contained up to 600 sticks of dynamite. Nearby Fremont Elementary was placed on lockdown, and parents were directed to pick their children up on the other side of the campus along Orange Street, Frasher said. Residents in the immediate area to the rear of the fire station were evacuated. The boxes were apparently dropped off at the fire station, but it's unclear who left them there. Fire station personnel were not at the location when the boxes were found, Frasher said.

Source: <http://www.signonsandiego.com/news/riverside/20060510-1456-e xplosives.html>

[[Return to top](#)]

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.